

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-326920

(43)Date of publication of application : 22.11.2001

(51)Int.Cl.

H04N 7/16
G09C 1/00
G09C 5/00
G11B 20/10
H04H 1/00
H04N 5/44
H04N 7/08
H04N 7/081
H04N 7/167

(21)Application number : 2000-149846

(71)Applicant : SONY CORP

(22)Date of filing : 17.05.2000

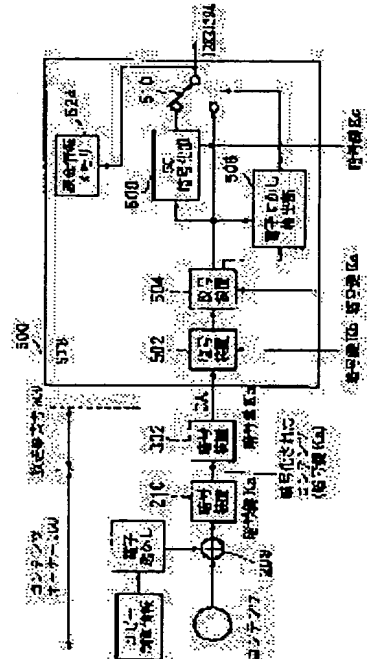
(72)Inventor : KORI TERUHIKO
FUJII ASAKO

(54) DATA DISTRIBUTION SYSTEM AND ITS METHOD, DATA RECEIVER, DATA SERVICE DEVICE AND ITS METHOD, AND DATA DELIVERY DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents distribution system with which a right holder can directly control the use of contents data without the aid of a broadcasting entrepreneur while the holder is in the state of capable of connecting a standard I/F and a contents processor.

SOLUTION: A contents owner 200 superposes copy control information by using a digital watermark, and provides the broadcasting entrepreneur 300 with encrypted contents data. The broadcasting entrepreneur 300 distributes by performing encryption for a conditional access. A set top box 500 which received the contents data firstly performs decoding for the conditional access, and secondly performs decoding by using an encryption key distributed by the contents owner 200. Then, the set copy control information is read by extracting digital watermark information, and thus an output from the set top box 500 is controlled.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-326920

(P2001-326920A)

(43)公開日 平成13年11月22日 (2001. 11. 22)

(51)Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 N 7/16		H 0 4 N 7/16	Z 5 C 0 2 5
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D 5 C 0 6 3
	5/00		5 C 0 6 4
G 1 1 B 20/10		G 1 1 B 20/10	H 5 D 0 4 4
H 0 4 H 1/00		H 0 4 H 1/00	F 5 J 1 0 4

審査請求 未請求 請求項の数34 O L (全 18 頁) 最終頁に続く

(21)出願番号 特願2000-149846(P2000-149846)

(22)出願日 平成12年5月17日(2000. 5. 17)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 郡 照彦

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72)発明者 藤井 麻子

アメリカ合衆国 ニュージャージー州 パー クリッジソニー ドライブ ソニー コーポレーション オブ アメリカ内

(74)代理人 100094053

弁理士 佐藤 隆久

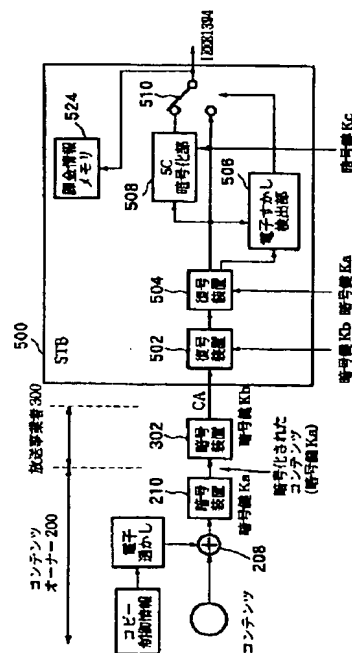
最終頁に続く

(54)【発明の名称】 データ配信システムとその方法、データ受信装置、データ提供装置とその方法およびデータ送出装置

(57)【要約】

【課題】標準的な I/F およびコンテンツ処理装置を接続可能な状態でありながら、放送事業者の手を介さずに権利者が直接コンテンツデータの使用を制御することができるコンテンツ配信システムを提供する。

【解決手段】コンテンツオーナー200は、コピー制御情報を電子透かしにより重畳し、さらに暗号化したコンテンツデータを放送事業者300に提供する。放送事業者300はコンディショナルアクセスのための暗号化を行なって配信する。これを受信したセットトップボックス500では、まずコンディショナルアクセスのための復号を行い、次にコンテンツオーナー200から配布された暗号鍵を用いて復号を行なう。そして、電子透かし情報を取り出して設定されているコピー制御情報を読み出し、これによりセットトップボックス500からの出力を制御する。



【特許請求の範囲】

【請求項 1】 所望のコンテンツデータに、当該コンテンツデータの使用状態を制御する第 1 の制御情報を付加し配信対象のデータとして提供するデータ提供手段と、前記提供された配信対象のデータに所定の第 2 の暗号化を行い、当該暗号化された配信対象のデータを送信するデータ送信手段と、

前記送信された暗号化された配信対象のデータを受信し、前記第 2 の暗号化の復号化を行い、該復号化された配信対象のデータより前記第 1 の制御情報を検出し、該検出された第 1 の制御情報に基づいて前記コンテンツデータの出力を制御するデータ受信手段とを有するデータ配信システム。

【請求項 2】 前記データ提供手段は、前記第 1 の制御情報を電子透かし情報として前記コンテンツデータに重畳し、該重畳されたコンテンツデータを配信対象のデータとして前記データ送信手段に提供し、

前記データ送信手段は、前記提供された配信対象のデータに所定の第 2 の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第 2 の暗号化の復号化を行い、該復号化された配信対象のデータより前記重畳された第 1 の制御情報を検出し、該検出された第 1 の制御情報に基づいて前記コンテンツデータの出力を制御する請求項 1 に記載のデータ配信システム。

【請求項 3】 前記データ提供手段は、前記第 1 の制御情報を電子透かし情報として重畳したコンテンツデータに所定の第 1 の暗号化を行い、当該暗号化されたデータを前記配信対象のデータとして前記データ送信手段に提供し、

前記データ送信手段は、前記提供された配信対象のデータに前記第 2 の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第 2 の暗号化の復号化を行い、前記第 1 の暗号化の復号化を行い前記電子透かし情報が重畳されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記重畳された第 1 の制御情報を検出し、該検出された情報に基づいて前記コンテンツデータの出力を制御する請求項 2 に記載のデータ配信システム。

【請求項 4】 前記データ送信手段は、前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第 2 の制御情報を付加し、当該第 2 の制御情報の付加された前記配信対象のデータに前記第 2 の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第 2 の暗号化の復号化を行い、前記第 2 の制御情報を検出し、前記復号化された

配信対象のデータに前記第 1 の暗号化の復号化を行い電子透かし情報が重畳されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記電子透かし情報として重畳された第 1 の制御情報を検出し、前記検出された第 1 の制御情報および第 2 の制御情報に基づいて前記コンテンツデータの出力を制御する請求項 3 に記載のデータ配信システム。

【請求項 5】 前記データ提供手段は、前記第 1 の制御情報を示す制御記述子を前記コンテンツデータに付加し、該制御記述子の付加されたコンテンツデータを配信対象のデータとして前記データ送信手段に提供し、前記データ送信手段は、前記提供された配信対象のデータに所定の第 2 の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第 2 の暗号化の復号化を行い、該復号化された配信対象のデータより前記付加された第 1 の制御情報を検出し、該検出された第 1 の制御情報に基づいて前記コンテンツデータの出力を制御する請求項 1 に記載のデータ配信システム。

【請求項 6】 前記データ送信手段は、前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第 2 の制御情報を付加し、当該第 2 の制御情報の付加された前記配信対象のデータに前記第 2 の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第 2 の暗号化の復号化を行い、前記第 2 情報を検出し、前記復号化された配信対象のデータに前記第 1 の暗号化の復号化を行い制御記述子が付加されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記制御記述子として付加された第 1 の制御情報を検出し、前記検出された第 1 の制御情報および第 2 の制御情報に基づいて前記コンテンツデータの出力を制御する請求項 5 に記載のデータ配信システム。

【請求項 7】 前記データ提供手段は、前記コンテンツデータをアナログ信号により出力する際の当該信号の使用状態を制御する第 3 の制御情報を、当該コンテンツデータに電子透かし情報として重畳し、該第 3 の制御情報の重畳されたコンテンツデータを前記配信対象のデータとして提供し、

前記データ送信手段は、前記提供された配信対象のデータに所定の第 2 の暗号化を行い、当該暗号化された配信対象のデータを送信し、

前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第 2 の暗号化の復号化を行い、該復号化された前記第 3 の制御情報が電子透かし情報として重畳された信号を、要求に応じてアナログ信号出力として出力する請求項 1 に記載のデータ配信システム。

10

20

30

40

50

【請求項 8】前記データ受信手段は、前記受信したコンテンツデータの使用状態に基づく、当該コンテンツデータの使用に対する課金に係わる情報を記憶する記憶手段をさらに有する請求項 1 に記載のデータ配信システム。

【請求項 9】所望のコンテンツデータに、当該コンテンツデータの権利者の指示に基づいて当該コンテンツデータの使用状態を制御する第 1 の制御情報を付加し配信対象のデータとして提供し、

前記提供された配信対象のデータに所定の第 2 の暗号化を行い、

当該暗号化された配信対象のデータを送信し、

任意の受信装置において前記送信された暗号化された配信対象のデータを受信し、

前記第 2 の暗号化の復号化を行い、

該復号化された配信対象のデータより前記第 1 の制御情報を検出し、

該検出された第 1 の制御情報に基づいて前記コンテンツデータの出力を制御するを有するデータ配信方法。

【請求項 10】前記第 1 の制御情報を電子透かし情報として前記コンテンツデータに重畳し、該重畳されたコンテンツデータを配信対象のデータとして提供し、

前記第 1 の制御情報の検出は、前記復号化された配信対象のデータより前記電子透かし情報を検出することにより行なう請求項 9 に記載のデータ配信方法。

【請求項 11】前記第 1 の制御情報を電子透かし情報として重畳したコンテンツデータに所定の第 1 の暗号化を行い、当該暗号化されたデータを前記配信対象のデータとして提供し、

前記第 2 の暗号化の復号化が行なわれたデータに対して、さらに、前記第 1 の暗号化の復号化を行い、前記電子透かし情報が重畳されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記重畳された第 1 の制御情報を検出する請求項 10 に記載のデータ配信方法。

【請求項 12】前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第 2 の制御情報を付加し、

当該第 2 の制御情報の付加された前記配信対象のデータに前記第 2 の暗号化を行い、

当該暗号化された配信対象のデータを送信し、

任意の受信装置において前記送信された暗号化された配信対象のデータを受信し、

前記第 2 の暗号化の復号化を行い、

前記第 2 の制御情報を検出し、

前記復号化された配信対象のデータに前記第 1 の暗号化の復号化を行い電子透かし情報が重畳されたコンテンツデータを生成し、

当該生成されたコンテンツデータより前記電子透かし情報として重畳された第 1 の制御情報を検出し、

前記検出された第 1 の制御情報および第 2 の制御情報に

10

基づいて前記コンテンツデータの出力を制御する請求項 11 に記載のデータ配信方法。

【請求項 13】前記第 1 の制御情報の付加は、当該第 1 の制御情報を示す制御記述子を前記コンテンツデータに付加することにより行い、

前記第 1 の制御情報の検出は、前記第 2 の暗号化の復号化が行なわれた配信対象のデータより当該付加された第 1 の制御情報を検出することにより行なう請求項 9 に記載のデータ配信方法。

20

【請求項 14】前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第 2 の制御情報を付加し、

当該第 2 の制御情報の付加された前記配信対象のデータに前記第 2 の暗号化を行い、

当該暗号化された配信対象のデータを送信し、

前記送信された暗号化された配信対象のデータを受信し、

前記第 2 の暗号化の復号化を行い、

前記第 2 情報を検出し、

前記復号化された配信対象のデータに前記第 1 の暗号化の復号化を行い制御記述子が付加されたコンテンツデータを生成し、

当該生成されたコンテンツデータより前記制御記述子として付加された第 1 の制御情報を検出し、

前記検出された第 1 の制御情報および第 2 の制御情報に基づいて前記コンテンツデータの出力を制御する請求項 13 に記載のデータ配信方法。

30

【請求項 15】前記コンテンツデータをアナログ信号により出力する際の当該信号の使用状態を制御する第 3 の制御情報を、当該コンテンツデータの権利者の指示に基づいて、当該コンテンツデータに電子透かし情報として重畳し、該第 3 の制御情報の重畳されたコンテンツデータを前記配信対象のデータとして提供し、

前記提供された配信対象のデータに所定の第 2 の暗号化を行い、

当該暗号化された配信対象のデータを送信し、

任意の受信装置において前記送信された暗号化された配信対象のデータを受信し、

前記第 2 の暗号化の復号化を行い、

40

少なくともアナログ信号出力が要求された場合には、該復号化された前記第 3 の制御情報が電子透かし情報として重畳された信号を出力する請求項 9 に記載のデータ配信方法。

【請求項 16】前記受信したコンテンツデータの使用状態に基づいて、当該コンテンツデータの使用に対する課金を行なう請求項 9 に記載のデータ配信方法。

【請求項 17】所望のコンテンツデータに、当該コンテンツデータの使用状態を制御する第 1 の制御情報を付加した配信対象のデータに、所定の第 2 の暗号化を行い送信される信号を受信するデータ受信装置であって、

50

前記送信された信号を受信する受信手段と、
前記受信した信号に対して前記第 2 の暗号化の復号化を行う第 2 の復号化手段と、
前記復号化された配信対象のデータより前記第 1 の制御情報を検出する第 1 の制御情報検出手段と、
前記検出された第 1 の制御情報に基づいて前記コンテンツデータの出力を制御する出力制御手段とを有するデータ受信装置。

【請求項 18】前記送信される信号は、前記第 1 の制御情報が付加されたコンテンツデータに対して、所定の第 1 の符号化を行い、さらに所定の第 2 の暗号化を行った信号であり、
前記第 2 の復号化手段で復号化されたデータに対して前記第 1 の暗号化の復号化を行なう第 1 の復号化手段をさらに有し、
前記第 1 の制御情報検出手段は、前記第 1 の復号化手段で復号化された結果の前記配信対象のデータより、当該第 1 の制御情報を検出する請求項 17 に記載のデータ受信装置。

【請求項 19】前記第 1 の復号化手段は、前記コンテンツデータの権利者により配布された所定の鍵データを用いて、前記復号化を行なう請求項 18 に記載のデータ受信装置。

【請求項 20】前記第 2 の復号化手段は、前記信号の送信者により配布された所定の鍵データを用いて、前記復号化を行なう請求項 19 に記載のデータ受信装置。

【請求項 21】前記第 1 の制御情報は電子透かし情報として前記コンテンツデータに重畳されており、
前記第 1 の制御情報検出手段は、前記復号化された配信対象のデータより前記電子透かし情報として重畳された第 1 の制御情報を検出する請求項 20 に記載のデータ受信装置。

【請求項 22】前記送信される信号は、前記第 1 の制御情報および当該コンテンツデータの使用状態を制御する第 2 の制御情報が付加されたコンテンツデータに対して、所定の第 1 の符号化を行い、さらに所定の第 2 の暗号化を行った信号であり、
前記復号化された配信対象のデータより前記第 2 の制御情報を検出する第 2 の制御情報検出手段と、
前記検出された第 1 の制御情報および第 2 の制御情報に基づいて、制御内容を決定する制御内容決定手段とをさらに有し、
前記出力制御手段は、前記決定された制御内容に従って、前記コンテンツデータの出力を制御する請求項 17 に記載のデータ受信装置。

【請求項 23】前記第 1 の制御情報は前記コンテンツデータの権利者により設定された情報であり、
前記第 2 の制御情報は前記信号の送信者により設定された情報であり、
前記制御内容決定手段は、前記検出された第 1 の制御情

報および第 2 の制御情報に基づいて、前記コンテンツデータの権利者の設定が、前記信号の送信者の設定よりも優先されるように、前記制御内容を決定する請求項 22 に記載のデータ受信装置。

【請求項 24】前記第 1 の制御情報は制御記述子として前記コンテンツデータに付加されており、
前記第 1 の制御情報検出手段は、前記復号化された配信対象のデータより前記制御記述子として付加された第 1 の制御情報を検出する請求項 20 に記載のデータ受信装置。

【請求項 25】前記送信される信号は、前記コンテンツデータに、さらに、当該コンテンツデータをアナログ信号により出力する際の当該信号の使用状態を制御する第 3 の制御情報が電子透かし情報として重畳されたデータに基づいた前記信号であり、
前記出力制御手段は、要求に応じてアナログ信号により前記コンテンツデータを出力する際には、前記第 3 の制御情報が電子透かし情報として重畳された信号を出力する請求項 17 に記載のデータ受信装置。

【請求項 26】前記受信したコンテンツデータの使用状態に基づく、当該コンテンツデータの使用に対する課金に係わる情報を記憶する記憶手段をさらに有する請求項 17 に記載のデータ受信装置。

【請求項 27】所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報を付加する制御情報付加手段と、
前記制御情報が付加されたコンテンツデータを、配信対象のデータとして提供するデータ提供装置。

【請求項 28】前記制御情報の付加されたコンテンツデータを、所定の方式により暗号化する暗号化手段をさらに有し、
前記暗号化されたコンテンツデータを提供する請求項 27 に記載のデータ提供装置。

【請求項 29】前記制御情報付加手段は、前記制御情報を、電子透かし情報として前記コンテンツデータに重畳する請求項 28 に記載のデータ提供装置。

【請求項 30】前記制御情報付加手段は、前記制御情報を、制御記述子として前記コンテンツデータに付加する請求項 28 に記載のデータ提供装置。

【請求項 31】前記コンテンツデータの権利者により指定された、当該コンテンツデータがアナログ信号として出力される際に当該信号の使用状態を制御するアナログ信号制御情報を、電子透かし情報として前記コンテンツデータに重畳するアナログ信号制御情報付加手段をさらに有し、
前記アナログ信号制御情報が重畳されたコンテンツデータを提供する請求項 27 に記載のデータ提供装置。

【請求項 32】所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデ

ータの使用状態を制御する制御情報を付加し、前記制御情報の付加されたコンテンツデータを所定の方式により暗号化し、該暗号化したコンテンツデータを配信対象のデータとして提供するデータ提供方法。

【請求項 33】前記暗号化されたコンテンツデータを復号化する鍵データは、配信された当該暗号化されたコンテンツデータを受信する受信装置にのみ提供する請求項 32 に記載のデータ提供方法。

【請求項 34】所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報が付加され、所定の方式により暗号化された配信対象のデータを、さらに所定の方式により暗号化する暗号化手段と、前記暗号化した配信対象のデータを任意の伝送路に送出する送出手段とを有するデータ送出装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、所望のコンテンツデータを適切に権利処理を行い配信することのできるデータ配信システムおよびデータ配信方法、配信されるコンテンツデータを受信し適切な権利処理を行なって利用可能に出力するデータ受信装置、コンテンツの権利者がその利用をコントロールできる状態で配信対象のコンテンツデータを提供するデータ提供装置およびデータ提供方法、および、その提供されたデータを送出するデータ送出装置に関する。

【0002】

【従来の技術】近年、衛星放送やCATVなどの種々の形態の放送や、いわゆる放送に限られないたとえばインターネットなどの通信ネットワークを介したデータ配信システムなどの、種々のコンテンツ配信システムが実現されている。そしてそのようなデータ配信システムにおいては、有料で配信されるコンテンツが大きな割合を占めるようになってきている。コンテンツを有料で配信する際の、コンテンツの使用をコントロールする方法としては、コンテンツを暗号化して送出し、受信機器側に暗号を解くためのライセンスを行うことによりコピーコントロールを行なうようにしている場合が多い。ライセンスによって、受信機器側の再生出力自体がコントロールされる。なお、このような観点で言えば、DVDなどのパッケージメディアを介したコンテンツの配信についても、同様のことが言える。

【0003】適切なコピーコントロールを行いながら所望のコンテンツを配信する従来のシステムについて、図 10～図 13 を参照して説明する。図 10 に示すコンテンツ配信システム 911 においては、まず、コンテンツの権利者であるコンテンツオーナー 920 が、暗号化されていないコンテンツを放送事業者 930 に渡す。放送事業者 930 は、暗号鍵 K b を用いてコンディショナル

アクセス (CA) のための暗号化を行い、放送網 940 に送出する。これを受信したセットトップボックス 950 は、予め契約などにより配布されている暗号鍵 K b を用いてコンディショナルアクセスのための暗号化を解く。そして、表示装置 970 との間で伝送を行なうための暗号化を行い、表示装置 970 に対して送出する。なお、セットトップボックス 500 と表示装置 700 との間の表示装置 I/F 600 は、たとえば IEEE 1394 インターフェイスなどが用いられる。その場合、セットトップボックス 500 は、復号化したコンテンツデータを 5C-DTCP 方式の暗号化を行なう。

【0004】図 10 に示したシステムにおける、コンテンツデータの使用の制御（以後、単にコピー制御と言う場合もある。）の処理について、図 11 を参照して詳細に説明する。まず、コピー制御の条件などは、通常コンテンツオーナー 920 が決定する。したがって、コンテンツオーナー 920 は、このコピー制御情報と、コンテンツデータとを放送事業者 930 に提供する。放送事業者 930 は、コンテンツオーナー 900 から受け取ったコピー制御情報を制御記述子に変換し、制御記述子付加部 932 においてコンテンツデータに付加する。そして、この制御記述子の付加されたコンテンツデータに対して、放送事業者 930 が、暗号装置 934 において、暗号鍵 K b を用いてコンディショナルアクセスのための暗号化を行い、セットトップボックス 950 に送出する。

【0005】セットトップボックス 950 においては、復号装置 952 でコンディショナルアクセスのための暗号化が復号化され、制御記述子検出部 954 においてコンテンツデータに付加された制御記述子が検出される。そして、たとえばこの制御記述子に、セットトップボックス 950 から暗号化したコンテンツデータを出力するように記載されていた場合には、制御記述子検出部 954 からの制御信号に基づいて、復号装置 952 からの出力を 5C 暗号化部 956 で暗号鍵 K c を用いて暗号化したデータを出力スイッチ 958 において選択し、セットトップボックス 950 より出力する。また、制御記述子に、セットトップボックス 950 から暗号化されていないコンテンツデータを出力してよい旨の記載があった場合には、制御記述子検出部 954 からの制御信号に基づいて、復号装置 952 からの出力を出力スイッチ 958 で選択し、セットトップボックス 950 より出力する。

【0006】この時に放送事業者 930 で使用される制御記述子の例を図 12 に示す。図 12 に示すディスクリプタにおいては、(1) の箇所に出力データに対するコピーコントロールタイプとして 5C を選択する旨の設定がなされている。また (2) の箇所にコピー制御情報である CGMS が記載されている。

【0007】このようなコンテンツ配信システム 911 においては、暗号化されていないコンテンツ (ソース)

であっても、放送時には暗号鍵K bのコンディショナルアクセスの暗号化によって守られ、受信後CAを解かれたあとも受信機から出力される際には暗号鍵K cで暗号化されて伝送されるので、コンテンツのセキュリティは保たれる。また、受信機と表示装置間の接続は放送サービスの形態に係わらず、5C-DTCP対応のIEEE 1394での標準化が可能であり、受信機と表示装置は標準のものをを用いることができる。

【0008】また、XCA(Extended Conditional Access)と呼ばれるコンテンツ配信システムを図13に示す。このビットストリーム化回路912においては、まず、コンテンツオーナー920が暗号鍵K aを用いて、コンテンツ自体に暗号をかけて放送事業者930に渡す。次に、放送事業者930は、暗号鍵K bを用いて、さらにコンディショナルアクセスのための暗号化を行い送出する。セットトップボックス950は、暗号鍵K bを用いてコンディショナルアクセスを解き、これをそのまま表示装置に送る。この状態でまだコンテンツは暗号化されている。そして、表示装置970において、内蔵される復号装置972により、暗号鍵K aを用いて暗号化を解き、復号化されたコンテンツを得る。

【0009】このコンテンツ配信システム912においては、最初に暗号化されたコンテンツは、途中の経路では一切暗号が解かれることなく伝送され、表示装置に伝送されて初めて暗号が復号化される仕組みになっている。したがって、伝送経路の装置や放送事業者に不正があるような場合でも、コンテンツの最終到着地である表示装置内でのみ最初の鍵K aによる暗号が復号化されるので安全性が高い。

【0010】

【発明が解決しようとする課題】しかしながら、図11を参照して説明した従来のシステムでは、コンテンツオーナーからデータが放送事業者に渡される際には、コンテンツデータも、コピー制御情報も、全く暗号化されていない状態で取り扱われる。その結果、放送事業者が制御記述子を間違えたり、載せるのを誤ったり、あるいは故意に変更したりすると、コンテンツオーナーが意図していた本来のコピー制御、すなわちコンテンツデータの使用の制御が行なえなくなるという問題がある。一方で、図13を参照して説明した従来のシステムにおいては、安全性が高い反面、表示装置が全て暗号鍵K aによる暗号を復号化できる機能を持つ必要があり、表示装置を標準化、共通化することができないという問題がある。

【0011】したがって本発明の目的は、受信機より後段の処理装置として標準的な装置を使用しながら、コンテンツオーナーが直接、所望のコピーコントロールを行なうことができるコンテンツ配信システムおよびコンテンツ配信方法を提供することにある。また本発明の他の目的は、そのようなコンテンツ配信システムにおいて用

いられ、配信されるコンテンツデータを受信し適切な権利処理を行なって利用可能に出力するデータ受信装置を提供することにある。また本発明の他の目的は、コンテンツの権利者がその利用をコントロールできる状態で配信対象のコンテンツデータを提供するデータ提供装置およびデータ提供方法を提供することにある。さらに本発明の他の目的は、そのように提供されたデータを送出するデータ送出装置を提供することにある。

【0012】

【課題を解決するための手段】前記課題を解決するために、本発明のデータ配信システムは、所望のコンテンツデータに、当該コンテンツデータの使用状態を制御する第1の制御情報を付加し配信対象のデータとして提供するデータ提供手段と、前記提供された配信対象のデータに所定の第2の暗号化を行い、当該暗号化された配信対象のデータを送信するデータ送信手段と、前記送信された暗号化された配信対象のデータを受信し、前記第2の暗号化の復号化を行い、該復号化された配信対象のデータより前記第1の制御情報を検出し、該検出された第1の制御情報に基づいて前記コンテンツデータの出力を制御するデータ受信手段とを有する。

【0013】好適には、前記データ提供手段は、前記第1の制御情報を電子透かし情報として前記コンテンツデータに重畳し、該重畳されたコンテンツデータを配信対象のデータとして前記データ送信手段に提供し、前記データ送信手段は、前記提供された配信対象のデータに所定の第2の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第2の暗号化の復号化を行い、該復号化された配信対象のデータより前記重畳された第1の制御情報を検出し、該検出された第1の制御情報に基づいて前記コンテンツデータの出力を制御する。

【0014】また好適には、前記データ提供手段は、前記第1の制御情報を電子透かし情報として重畳したコンテンツデータに所定の第1の暗号化を行い、当該暗号化されたデータを前記配信対象のデータとして前記データ送信手段に提供し、前記データ送信手段は、前記提供された配信対象のデータに前記第2の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第2の暗号化の復号化を行い、前記第1の暗号化の復号化を行い前記電子透かし情報が重畳されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記重畳された第1の制御情報を検出し、該検出された情報に基づいて前記コンテンツデータの出力を制御する。

【0015】特定的には、前記データ送信手段は、前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第2の制御情報を付加し、当該第

10

20

30

40

50

2の制御情報の付加された前記配信対象のデータに前記第2の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第2の暗号化の復号化を行い、前記第2の制御情報を検出し、前記復号化された配信対象のデータに前記第1の暗号化の復号化を行い電子透かし情報が重畳されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記電子透かし情報として重畳された第1の制御情報を検出し、前記検出された第1の制御情報および第2の制御情報に基づいて前記コンテンツデータの出力を制御する。

【0016】また特定のには、前記データ提供手段は、前記第1の制御情報を示す制御記述子を前記コンテンツデータに付加し、該制御記述子の付加されたコンテンツデータを配信対象のデータとして前記データ送信手段に提供し、前記データ送信手段は、前記提供された配信対象のデータに所定の第2の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第2の暗号化の復号化を行い、該復号化された配信対象のデータより前記付加された第1の制御情報を検出し、該検出された第1の制御情報に基づいて前記コンテンツデータの出力を制御する。

【0017】また好適には、前記データ送信手段は、前記提供された配信対象のデータに、当該コンテンツデータの使用状態を制御する第2の制御情報を付加し、当該第2の制御情報の付加された前記配信対象のデータに前記第2の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第2の暗号化の復号化を行い、前記第2の制御情報を検出し、前記復号化された配信対象のデータに前記第1の暗号化の復号化を行い制御記述子が付加されたコンテンツデータを生成し、当該生成されたコンテンツデータより前記制御記述子として付加された第1の制御情報を検出し、前記検出された第1の制御情報および第2の制御情報に基づいて前記コンテンツデータの出力を制御する。

【0018】さらに好適には、前記データ提供手段は、前記コンテンツデータをアナログ信号により出力する際の当該信号の使用状態を制御する第3の制御情報を、当該コンテンツデータに電子透かし情報として重畳し、該第3の制御情報の重畳されたコンテンツデータを前記配信対象のデータとして提供し、前記データ送信手段は、前記提供された配信対象のデータに所定の第2の暗号化を行い、当該暗号化された配信対象のデータを送信し、前記データ受信手段は、前記送信された暗号化された配信対象のデータを受信し、前記第2の暗号化の復号化を行い、該復号化された前記第3の制御情報が電子透かし情報として重畳された信号を、要求に応じてアナログ信号出力として出力する。好適には、前記データ受信手段

は、前記受信したコンテンツデータの使用状態に基づく、当該コンテンツデータの使用に対する課金に係わる情報を記憶する記憶手段をさらに有する。

【0019】また、本発明に係わるデータ配信方法は、所望のコンテンツデータに、当該コンテンツデータの権利者の指示に基づいて当該コンテンツデータの使用状態を制御する第1の制御情報を付加し配信対象のデータとして提供し、前記提供された配信対象のデータに所定の第2の暗号化を行い、当該暗号化された配信対象のデータを送信し、任意の受信装置において前記送信された暗号化された配信対象のデータを受信し、前記第2の暗号化の復号化を行い、該復号化された配信対象のデータより前記第1の制御情報を検出し、該検出された第1の制御情報に基づいて前記コンテンツデータの出力を制御する。

【0020】また、本発明に係わるデータ受信装置は、所望のコンテンツデータに、当該コンテンツデータの使用状態を制御する第1の制御情報を付加した配信対象のデータに、所定の第2の暗号化を行い送信される信号を受信するデータ受信装置であって、前記送信された信号を受信する受信手段と、前記受信した信号に対して前記第2の暗号化の復号化を行う第2の復号化手段と、前記復号化された配信対象のデータより前記第1の制御情報を検出する第1の制御情報検出手段と、前記検出された第1の制御情報に基づいて前記コンテンツデータの出力を制御する出力制御手段とを有する。

【0021】また、本発明に係わるデータ提供装置は、所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報を付加する制御情報付加手段と、前記制御情報が付加されたコンテンツデータを、配信対象のデータとして提供する。

【0022】また、本発明に係わるデータ提供方法は、所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報を付加し、前記制御情報の付加されたコンテンツデータを所定の方式により暗号化し、該暗号化したコンテンツデータを配信対象のデータとして提供する。

【0023】また、本発明に係わるデータ送出装置は、所望のコンテンツデータに、当該コンテンツデータの権利者により指定された当該コンテンツデータの使用状態を制御する制御情報が付加され、所定の方式により暗号化された配信対象のデータを、さらに所定の方式により暗号化する暗号化手段と、前記暗号化した配信対象のデータを任意の伝送路に送出する送出手段とを有する。

【0024】

【発明の実施の形態】本発明の実施の形態を図1～図9を参照して説明する。

【0025】全体構成

まず、本実施の形態のコンテンツ配信システムの全体構成について、図1を参照して説明する。図1は、本実施の形態のコンテンツ配信システム100の全体概略構成を示す図である。コンテンツ配信システム100は、コンテンツオーナー200、放送事業者300、放送網400、セットトップボックス500、表示装置I/F600および表示装置700を有する。

【0026】まず、各部の構成について説明する。コンテンツオーナー200は、配信対象のコンテンツの権利者であり、配信対象のコンテンツを所望の暗号鍵K_aを用いて暗号化し、暗号化された状態のコンテンツを放送事業者300に提供する。本実施の形態においては、コンテンツは、たとえばテレビプログラムや映画などの、映像および音声を含むコンテンツとする。なお、ここで言う暗号化とは、コンテンツデータそのもの、あるいはコンテンツオーナー200が要望する任意の付加データなどを、暗号鍵K_aなしでは何ら変更したり読み出したり使用したりすることができない状態にすることを広く指すものとする。したがって、具体的には、実際にコンテンツデータを暗号化する場合、付加データを電子透かしなどの形態で重畳する場合などが含まれる。なお、実際の具体的な処理内容については、後のより具体的な構成の説明の際に説明する。

【0027】放送事業者300は、コンテンツオーナー200より提供された暗号化された状態のコンテンツに、さらに暗号鍵K_bを用いてコンディショナルアクセスのための暗号化を行い、放送網400を介して配信する。

【0028】放送網400は、デジタル地上波放送、デジタル衛星放送、CATVあるいはインターネットなどの通信ネットワークを介した任意のデータ配信システムなどを含む、任意のデータ配信手段であり、放送事業者300により送出されたコンテンツデータを任意の利用者に配信する。

【0029】セットトップボックス500は、たとえば各利用者の家庭などに設けられ、利用者の操作に基づいて、放送網400を介して放送事業者300より送出されたデータを受信する受信装置である。セットトップボックス500は、利用者により選択されたコンテンツデータを受信すると、たとえば予め契約などに基づいて配布される暗号鍵K_aを用いて復号化する。そして、予め設定されている暗号鍵K_cを用いてその復号化されたコンテンツデータを再度暗号化し、表示装置I/F600に送出する。本実施の形態においては、セットトップボックス500と表示装置700とは、IEEE1394をインターフェイスとして接続されており、セットトップボックス500はIEEE1394に規定されている5C暗号化方式によりコンテンツデータを再度暗号化する。

【0030】表示装置I/F600は、セットトップボ

ックス500と表示装置700との間の接続手段であり、前述したように本実施の形態ではIEEE1394である。

【0031】表示装置700は、表示装置I/F600を介してセットトップボックス500より入力される暗号化されたコンテンツデータを、予め設定されている暗号鍵K_cを用いて復号化し、使用者が視聴可能に表示する。

【0032】次に、このような構成のコンテンツ配信システム100の全体の動作の概略について説明する。まず、配信対象のコンテンツは、その権利者であるコンテンツオーナー200により暗号鍵K_aを用いて暗号化された上で放送事業者300に受け渡され、放送事業者300によりさらに暗号鍵K_bを用いてコンディショナルアクセスのための暗号化をされ、放送網400に送出される。

【0033】放送網400に送出されたデータは、これを視聴しようとして選択した視聴者（コンテンツの使用者）により、具体的にはその使用者の操作されるセットトップボックス500により実質的に受信され、内部の復号装置によりまずコンディショナルアクセスのための暗号が復号化される。この時の暗号鍵K_aは、使用者が予め放送事業者300と受信契約を結ぶ際に、たとえばICカードのようなセキュアな記録媒体などの形態で提供される。

【0034】復号化されたコンテンツデータは、予め設定された暗号鍵K_cを用いてIEEE1394の5C方式により再度暗号化され、表示装置700に送出される。そして、表示装置700において復号化され、使用者が視聴可能に表示される。なお、視聴者がセットトップボックス500に対して行なう、受信するコンテンツデータの選択や、セットトップボックス500から表示装置700へのコンテンツデータの送出などの操作は、セットトップボックス500内の課金情報メモリに逐次記憶され、コンテンツ受信に伴う課金に用いられる。

【0035】このように、コンテンツ配信システム100においては、コンテンツオーナー200自体が配信対象のコンテンツに実質的に暗号化を行なっており、またその暗号化は、使用者のセットトップボックス500まで復号されない構成となっている。したがって、たとえば使用者側におけるコンテンツデータの再生やコピーを制御するコントロール情報を暗号化してコンテンツデータに重畳しておけば、コンテンツオーナー200自身が使用者側におけるコンテンツデータの使用をコントロールすることができる。すなわち、理由の如何を問わず、放送事業者300によるコンテンツの使用状態や使用条件などが変更されてしまうことを防ぐことができる。

【0036】また、コンテンツ配信システム100においては、コンテンツの使用をそのようなコンテンツオーナー200のコントロールの範囲内に置きながら、セッ

トトップボックス 500 と表示装置 700 との間は標準インターフェイスを用いることができる。また、表示装置 700 もそのインターフェイスに対応した標準的な装置を用いることができる。

【0037】 具体的適用例

以上、本発明に係わるコンテンツ配信システム 100 の全体の構成の概略を説明したが、以下は、より具体的な構成例、具体的な適用形態について、第 1 の具体例～第 5 の具体例として説明する。なお、放送網 400、表示装置 I/F 600 および表示装置 700 はいずれも標準的なものなので、以下の説明においては、図面上へのその記載および説明を省略する。

【0038】 第 1 の具体例

コンテンツ配信システム 100 の第 1 の具体的な適用例を、図 2 を参照して説明する。第 1 の具体例としては、コンテンツオーナー 200 がコンテンツの使用を制御する制御情報を電子透かし形態でコンテンツデータに重畳して配信し、これにより使用者に受信されたコンテンツデータの使用が制御されるシステムを例示する。図 2 は、コンテンツ配信システム 100 の第 1 の具体的構成の、コンテンツオーナー 200 ～セットトップボックス 500 までの構成を示す図である。

【0039】 図 2 に示す第 1 の具体的構成においては、コンテンツオーナー 200 は、電子透かし重畳部 208 を有しており、セットトップボックス 500 において有効となるコンテンツの使用を制御するコピー制御情報を、電子透かしの形態でコンテンツデータに重畳する。さらにコンテンツオーナー 200 は、暗号装置 210 を有しており、電子透かしの重畳されたコンテンツデータを、暗号鍵 K_a を用いて暗号化する。そして、この暗号化されたコンテンツデータを放送事業者 300 に渡す。

【0040】 放送事業者 300 は、暗号装置 302 を有しており、コンテンツオーナー 200 から入力されたコンテンツデータに対して、暗号鍵 K_b を用いてさらにコンディショナルアクセスのための暗号化を行い送出する。

【0041】 セットトップボックス 500 は、2 個の復号装置 502、復号装置 504、電子透かし検出部 506、5C 暗号化部 508、出力スイッチ 510 および課金情報メモリ 524 を有する。復号装置 502 は、放送事業者 300 より受信した暗号化された信号を、暗号鍵 K_b を用いて復号する。すなわち、コンディショナルアクセスのための暗号化を復号する。復号した信号は、コンテンツオーナー 200 により暗号化された信号であり、まだ使用することはできない。

【0042】 復号装置 504 は、復号装置 502 において復号された信号に対して、さらに、暗号鍵 K_a を用いて復号化し、復号化した信号を電子透かし検出部 506、5C 暗号化部 508 および出力スイッチ 510 に出力する。復号装置 504 において復号化された信号は、

ベースバンドのコンテンツデータにコピー制御情報が電子透かしとして重畳されている信号である。電子透かし検出部 506 は、復号装置 504 において復号された信号より、電子透かしとして重畳されているコピー制御情報を検出し、これに基づいてセットトップボックス 500 から出力する信号を制御する信号、具体的には出力スイッチ 510 を制御する信号を生成して、出力スイッチ 510 に印加する。5C 暗号化部 508 は、復号装置 504 において復号された信号を、暗号鍵 K_c を用いて 5C 方式により暗号化し、出力スイッチ 510 に印加する。

【0043】 出力スイッチ 510 は、電子透かし検出部 506 より印加される制御信号に基づいて、セットトップボックス 500 からの出力信号として、復号装置 504 より出力される暗号化されていないコンテンツデータ、あるいは、5C 暗号化部 508 で暗号化されたコンテンツデータのいずれかを選択し、セットトップボックス 500 より出力する。課金情報メモリ 524 は、実質的にセットトップボックス 500 より出力される信号を検出することにより、あるいは、IEEE 1394 を介して表示装置 700 より入力される情報を監視することにより、コンテンツデータの使用に伴う課金に係わる情報を検出し、これを記憶しておく。課金情報メモリ 524 に記憶された情報は、適宜所定の決済機関に送信され、課金処理が行なわれる。

【0044】 このようなセットトップボックス 500 においては、復号装置 502 で放送事業者 300 により施されたコンディショナルアクセスのための暗号化が復号化され、復号装置 504 でコンテンツオーナー 200 自身が施した暗号化が復号化され、その復号化されたコンテンツデータより、電子透かし検出部 506 において、電子透かしとして重畳されているコンテンツオーナー 200 により付加されたコピー制御情報が検出される。そして、たとえばこのコピー制御情報に、セットトップボックス 500 から暗号化したコンテンツデータを出力するように記載されていた場合には、電子透かし検出部 506 からの制御信号に基づいて、復号装置 504 からの出力を 5C 暗号化部 508 で暗号鍵 K_c を用いて暗号化したデータを出力スイッチ 510 において選択し、セットトップボックス 500 より図示せぬ表示装置に対して出力する。また、コピー制御情報に、セットトップボックス 500 から暗号化されていないコンテンツデータを出力してよい旨の記載があった場合には、電子透かし検出部 506 からの制御信号に基づいて、復号装置 504 からの出力を出力スイッチ 510 で選択し、セットトップボックス 500 より出力する。

【0045】 このように、第 1 の具体例においては、コンテンツオーナー 200 が電子透かしという形態でコピー制御情報をコンテンツデータに重畳し、さらに暗号化を行なっており、放送事業者 300 の手を介することな

く、コンテンツオーナー 200 自身が受信側の出力を直接制御することができる。

【0046】第2の具体例

コンテンツ配信システム 100 の第 2 の具体的な適用例を、図 3 を参照して説明する。第 2 の具体例は、第 1 の具体例におけるコンテンツオーナー 200 の暗号装置 210 を無くし、暗号化処理を省略した構成である。またこれに伴って、セットトップボックス 500 においても、復号装置 504 が省略された構成となっている。

【0047】そのような構成においては、コンテンツオーナー 200 は、電子透かし重畳部 208 においてコピー制御情報を電子透かしの形態で重畳し、その状態のコンテンツデータをそのまま、すなわち暗号化せずに放送事業者 300 に提供する。そして放送事業者 300 においては、これを暗号装置 302 でコンディショナルアクセスのための暗号化を行なって送出する。送出された信号を受信したセットトップボックス 500 においては、復号装置 502 でコンディショナルアクセスのための暗号化を復号化することにより、直ちに何ら暗号化されていないコンテンツデータが得られ、これより電子透かし検出部 506 において、電子透かしとして重畳されているコピー制御情報を検出し、これにより出力スイッチ 510 を制御する。5C 暗号化部 508、出力スイッチ 510 および図示せぬ課金情報メモリなどの動作は、第 1 の具体例と同じである。

【0048】このように、第 2 の具体例においては、コンテンツオーナー 200 における暗号装置 210 およびセットトップボックス 500 の復号装置 504 が省略されているため、各装置の構成を簡単にすることができる。このような構成においては、コンテンツオーナー 200 の暗号装置 210 による暗号化処理がなくなるため、放送事業者 300 には暗号化されていない状態のコンテンツデータが渡されることになるが、セットトップボックス 500 の出力はあくまでも電子透かし情報により制御されており、また、電子透かしデータが重畳されているため不正利用された場合のトレースが可能であることなどから、不正利用される可能性は低いと言える。このような条件でよければ、構成の簡単なこの第 2 の具体例が有効である。

【0049】第3の具体例

コンテンツ配信システム 100 の第 3 の具体的な適用例を、図 4 および図 5 を参照して説明する。第 3 の具体例は、放送事業者 300 においてコンテンツオーナー 200 が付加するのは別の独自の制御記述子を付加するようにした構成である。

【0050】具体的には、コンテンツオーナー 200 における処理は、第 1 の具体例の処理と同じであり、まず、セットトップボックス 500 において有効となるコンテンツの使用を制御するコピー制御情報を、電子透かしの形態でコンテンツデータに重畳する。次に、暗号装

置 210 において、電子透かしの重畳されたコンテンツデータを、暗号鍵 K a を用いて暗号化し、この暗号化されたコンテンツデータを放送事業者 300 に渡す。

【0051】放送事業者 300 は、コンテンツオーナー 200 から渡された暗号化されたコンテンツデータに対して、制御記述子付加部 306 において、独自の制御記述子を付加し、暗号装置 302 において暗号鍵 K b を用いて暗号化して送出する。

【0052】これを受信したセットトップボックス 500 は、復号装置 502 において放送事業者 300 により行なわれたコンディショナルアクセスのための暗号化を暗号鍵 K b を用いて復号する。この復号された信号より、制御記述子検出部 512 において、放送事業者 300 が付加した制御記述子が検出され、判定制御装置 514 に出力される。また、復号装置 502 で復号された信号は、さらに復号装置 504 において、暗号鍵 K a を用いて復号される。この復号された信号より、電子透かし検出部 506 において、コンテンツオーナー 200 が電子透かしの形態で重畳したコピー制御情報が検出され、判定制御装置 514 に出力される。

【0053】判定制御装置 514 は、電子透かし検出部 506 から入力されるコンテンツオーナー 200 により設定されたコピー制御情報、および、制御記述子検出部 512 から入力される放送事業者 300 により設定された制御記述子に基づいて、受信したコンテンツデータの使用を制御する判定を行い、その判定に基づいて出力データを制御する。ここで、コピー制御情報および制御記述子には、各々セットトップボックス 500 からコンテンツデータを出力する際に、5C 暗号化して伝送するか、暗号化せずに伝送するかの設定が行なわれているものとする。その場合、判定制御装置 514 はたとえば図 5 に示すようなフローチャートに従って判定を行なう。

【0054】すなわち、判定を開始すると（ステップ S10）、まず、電子透かし検出部 506 から入力されるコピー制御情報を参照して、5C 暗号化の設定が行なわれているか否かを判定する（ステップ S11）。そして、5C 暗号化の設定が行なわれていた場合には、出力スイッチ 510 に 5C 暗号化部 508 の出力を選択するような制御信号を出力することにより、セットトップボックス 500 から 5C 暗号化したコンテンツデータを出力させる（ステップ S12）。

【0055】電子透かし検出部 506 から入力されるコピー制御情報に、5C 暗号化の設定が行なわれていなかった場合には（ステップ S11）、制御記述子検出部 512 から入力される制御記述子を参照して、5C 暗号化の設定が行なわれているか否かを判定する（ステップ S13）。そして、5C 暗号化の設定が行なわれていた場合には、コピー制御情報において設定がなされていた場合と同様に、出力スイッチ 510 に 5C 暗号化部 508 の出力を選択するような制御信号を出力し、セットトッ

ブボックス 500 から 5C 暗号化したコンテンツデータを出力させる (ステップ S12)。

【0056】制御記述子検出部 512 から入力される制御記述子にも、5C 暗号化の設定が行なわれていなかった場合には (ステップ S13)、判定制御装置 514 は、出力スイッチ 510 に、復号装置 504 からの出力を選択するような制御信号を出力し、セットトップボックス 500 から暗号化されていないコンテンツデータを出力させる (ステップ S14)。

【0057】このように、第 3 の具体例においては、コンテンツオーナー 200 および放送事業者 300 が、各々独自にコンテンツデータの使用をコントロールする設定を行なうことができる。そして、どちらの設定をどのように優先させて、どのようなコントロールを行なうかは、判定制御装置 514 に設定するアルゴリズムを変えることで任意に設定することができる。そして、たとえば図 5 に示したようなアルゴリズムを採用することにより、放送事業者 300 による設定よりもコンテンツオーナー 200 による設定を優先して実行するようにすることができる。

【0058】第 4 の具体例

コンテンツ配信システム 100 の第 4 の具体的な適用例を、図 6 および図 7 を参照して説明する。第 4 の具体例は、第 3 の具体例と同様の構成であるが、コンテンツオーナー 200 によるコピーコントロールを、電子透かしをコンテンツデータに重畳することにより行なうのではなく、放送事業者 300 と同様に、制御記述子をコンテンツデータに付加することにより行なうようにしたものである。

【0059】すなわち、コンテンツオーナー 200 は、セットトップボックス 500 において有効となるコンテンツの使用を制御するコピー制御情報を、制御記述子付加部 212 において、制御記述子 (制御記述子 1) の形態でコンテンツデータに付加する。そして、その制御記述子の付加されたコンテンツデータに対して、暗号装置 210 において暗号鍵 K a を用いて暗号化し、暗号化されたコンテンツデータを放送事業者 300 に渡す。放送事業者 300 は、コンテンツオーナー 200 から渡された暗号化されたコンテンツデータに対して、制御記述子付加部 306 において、独自の制御記述子 (制御記述子 2) を付加し、暗号装置 302 において暗号鍵 K b を用いて暗号化して送出する。

【0060】これを受信したセットトップボックス 500 は、復号装置 502 において放送事業者 300 により行なわれたコンディショナルアクセスのための暗号化を暗号鍵 K b を用いて復号する。この復号された信号より、制御記述子 2 検出部 512 において、放送事業者 300 が付加した制御記述子 2 を検出し、判定制御装置 514 に出力する。また、復号装置 502 で復号された信号は、さらに復号装置 504 において、暗号鍵 K a を用

いて復号される。そしてこの復号された信号より、制御記述子 1 検出部 516 において、コンテンツオーナー 200 が付加した制御記述子 1 を検出し、判定制御装置 514 に出力する。

【0061】判定制御装置 514 は、制御記述子 1 検出部 516 から入力されるコンテンツオーナー 200 により設定された制御記述子 1、および、制御記述子 2 検出部 512 から入力される放送事業者 300 により設定された制御記述子 2 に基づいて、受信したコンテンツデータの使用を制御する判定を行い、その判定に基づいて出力データを制御する。ここで、制御記述子 1 および制御記述子 2 には、各々セットトップボックス 500 からコンテンツデータを出力する際に、5C 暗号化して伝送するか、暗号化せずに伝送するかの設定が行なわれているものとする。その場合、判定制御装置 514 はたとえば図 7 に示すようなフローチャートに従って判定を行なう。

【0062】すなわち、判定を開始すると (ステップ S20)、まず、制御記述子 1 検出部 516 から入力される制御記述子 1 を参照して、5C 暗号化の設定が行なわれているか否かを判定する (ステップ S21)。そして、5C 暗号化の設定が行なわれていた場合には、出力スイッチ 510 に 5C 暗号化部 508 の出力を選択するような制御信号を出力することにより、セットトップボックス 500 から 5C 暗号化したコンテンツデータを出力させる (ステップ S22)。

【0063】制御記述子 1 検出部 516 から入力される制御記述子 1 に、5C 暗号化の設定が行なわれていなかった場合には (ステップ S21)、制御記述子 2 検出部 512 から入力される制御記述子 2 を参照して、5C 暗号化の設定が行なわれているか否かを判定する (ステップ S23)。そして、5C 暗号化の設定が行なわれていた場合には、制御記述子 1 において設定がなされていた場合と同様に、出力スイッチ 510 に 5C 暗号化部 508 の出力を選択するような制御信号を出力し、セットトップボックス 500 から 5C 暗号化したコンテンツデータを出力させる (ステップ S22)。

【0064】制御記述子 2 検出部 512 から入力される制御記述子 2 にも、5C 暗号化の設定が行なわれていなかった場合には (ステップ S23)、判定制御装置 514 は、出力スイッチ 510 に、復号装置 504 からの出力を選択するような制御信号を出力し、セットトップボックス 500 から暗号化されていないコンテンツデータを出力させる (ステップ S24)。

【0065】このように、第 4 の具体例においては、コンテンツオーナー 200 および放送事業者 300 は、ともに制御記述子を付加するという形態で、各々独自にコンテンツデータの使用をコントロールする設定を行なうことができる。そして、どちらの設定をどのように優先させて、どのようなコントロールを行なうかは、判定制

御装置 514 に設定するアルゴリズムを変えることで任意に設定することができる。そして、たとえば図 7 に示したようなアルゴリズムを採用することにより、放送事業者 300 による設定よりもコンテンツオーナー 200 による設定を優先して実行するようにすることができる。

【0066】第 5 の具体例

コンテンツ配信システム 100 の第 5 の具体的な適用例を、図 8 を参照して説明する。第 5 の具体例は、セットトップボックス 500 からのアナログの出力に対して、適切にコピーコントロールが行なえるようにしたものである。

【0067】この場合、まずコンテンツオーナー 200 は、設定したいコピー制御情報を、電子透かし重畳部 208 において、電子透かしの形態でコンテンツデータに重畳する。この電子透かし情報は、セットトップボックス 500 からのアナログ出力のコピープロテクションに用いられる。そしてコンテンツオーナー 200 は、その電子透かし情報の重畳されたコンテンツデータに対して、暗号装置 210 において暗号鍵 K a を用いて暗号化する。この、暗号化されたコンテンツデータと、先のコピー制御情報の両方を、コンテンツオーナー 200 は放送事業者 300 に渡す。

【0068】放送事業者 300 は、コンテンツオーナー 200 から渡されたコピー制御情報を制御記述子に変換した後、これを、制御記述子付加部 306 において、コンテンツオーナー 200 から渡された暗号化されたコンテンツデータに付加し、暗号装置 302 において暗号鍵 K b を用いて暗号化して送出する。

【0069】これを受信したセットトップボックス 500 は、復号装置 502 において放送事業者 300 により行なわれたコンディショナルアクセスのための暗号化を暗号鍵 K b を用いて復号する。この復号された信号より、制御記述子検出部 512 において、コンテンツオーナー 200 からの指示により放送事業者 300 が付加した制御記述子を検出し、出力スイッチ 510 を制御する制御信号を生成して出力スイッチ 510 に印加する。また、復号装置 502 で復号された信号は、さらに復号装置 504 において、暗号鍵 K a を用いて復号される。この復号化された信号は、5C 暗号化部 508 において 5C 暗号化されて、あるいは、直接、出力スイッチ 510 に印加され、出力スイッチ 510 でいずれかが選択してデジタル出力として出力される。一方、復号装置 502 で復号された信号は、アナログ信号エンコーダ 518 に入力されて、ここでアナログ信号に変換されて、セットトップボックス 500 より出力される。

【0070】このように、第 5 の具体例においては、特に、セットトップボックス 500 より、電子透かしにより著作権保護情報が重畳された適切に権利処理されたアナログ信号を出力することができる。したがって、アナ

ログ信号出力を必要とする場合には好適である。

【0071】なお、図 8 に示した構成においては、コンテンツオーナー 200 が要求するコピー制御情報を、放送事業者 300 が制御記述子に変換してコンテンツデータに付加している。放送事業者 300 が十分信頼のおける機関であれば、このような構成として何ら問題は無い。しかし、何らかの理由でコンテンツオーナー 200 が自ら設定を行う場合には、第 3 の具体例の場合と同様に、制御記述子の設定もコンテンツオーナー 200 が行なうようにしてよい。

【0072】第 6 の具体例

コンテンツ配信システム 100 の第 6 の具体的な適用例を、図 9 を参照して説明する。第 6 の具体例は、セットトップボックス 500 からのデジタル出力を、モニタ接続用の DVI (Digital Visual Interface) およびその著作権保護された出力 (DVI-CP) のいずれかとし、また、アナログ出力を ON/OFF できるようにしたものである。

【0073】この場合、コンテンツオーナー 200 は、電子透かし重畳部 208 において、設定したいコピー制御情報を電子透かしの形態でコンテンツデータに重畳し、暗号装置 210 において、その電子透かし情報の重畳されたコンテンツデータを暗号鍵 K a を用いて暗号化し、暗号化されたコンテンツデータを、放送事業者 300 に渡す。

【0074】放送事業者 300 は、制御記述子付加部 306 において、独自の制御記述子をコンテンツオーナー 200 から渡された暗号化されたコンテンツデータに付加した後、暗号装置 302 において暗号鍵 K b を用いてコンディショナルアクセスのための暗号化を行い、送出する。

【0075】これを受信したセットトップボックス 500 は、復号装置 502 において、放送事業者 300 により行なわれたコンディショナルアクセスのための暗号化を暗号鍵 K b を用いて復号し、制御記述子検出部 512 において、この復号された信号より放送事業者 300 が付加した制御記述子を検出し、判定制御装置 514 に出力する。また、復号装置 502 で復号された信号は、さらに復号装置 504 において、暗号鍵 K a を用いて復号され、この復号された信号より、電子透かし検出部 506 において、コンテンツオーナー 200 が電子透かしの形態で重畳したコピー制御情報が検出され、判定制御装置 514 に出力される。

【0076】判定制御装置 514 は、電子透かし検出部 506 から入力されるコンテンツオーナー 200 により設定されたコピー制御情報、および、制御記述子検出部 512 から入力される放送事業者 300 により設定された制御記述子に基づいて、受信したコンテンツデータの使用を制御する判定を行い、その判定に基づいて出力データを制御する。具体的には、判定制御装置 514 は、

10

20

30

40

50

セットトップボックス 500 からのデジタル出力として、ベースバンドデータの出力を行なうか、DVI-C Pにより暗号化されたデータを出力するか判定、および、アナログ出力を行なうか否かの判定を行ない、各々その判定結果に基づく制御信号を、出力スイッチ 510 およびアナログ出力スイッチ 522 に出力する。

【0077】また、復号装置 504 において復号化された信号は、暗号化部 520 において DVI-C P に暗号化されて、あるいは、直接、出力スイッチ 510 に印加され、出力スイッチ 510 でいずれかが選択してデジタル出力として出力される。一方、復号装置 504 で復号された信号は、アナログ信号エンコーダ 518 に入力されて、ここでアナログ信号に変換されて、アナログ出力スイッチ 522 に印加され、判定制御装置 514 の制御に基づいてアナログ出力スイッチ 522 において選択され、アナログ出力として出力される。

【0078】このように、第 6 の具体例においては、セットトップボックス 500 から、DVI により、RGB ベースバンド信号あるいは符号化された信号として、デジタル映像信号を出力することができる。また、電子透かしにより著作権保護情報が重畳された適切に権利処理されたアナログ信号を、選択的に出力することができる。

【0079】変形例

なお、本発明は本実施の形態に限られるものではなく、任意好適な種々の変更が可能である。たとえば、コンテンツ配信システム 100 においてセットトップボックス 500 に接続されて利用される装置は、映像信号を表示する表示装置としたが、これに限られるものではなく、任意の画像処理装置を接続するようにしてよい。たとえば、出力されるデータを記録する記録装置を接続してもよいし、出力されるデータを伝送する伝送装置などを接続してもよい。また、セットトップボックス 500 の出力 I/F も、前述した実施の形態中で示した IEEE 1394 および DVI に限られるものではなく、任意の I/F を用いてよい。

【0080】また、放送事業者 300 とセットトップボックス 500 との間でデータを伝送する手段は、放送手段に限られるものではなく、任意の情報伝送手段を適用してよい。また、いわゆる放送に限られるものではなく、セットトップボックス 500 からの要求に応じて所望のコンテンツデータを要求のあったセットトップボックス 500 に送信するような伝送手段であってもよい。

【0081】また、本実施の形態においては、配信されるコンテンツは映像信号およびオーディオ信号を含むビデオ信号としたが、これに限られるものではなく、任意のコンテンツデータの配信に適用してよい。たとえば、オーディオデータ、静止画像データ、ゲームソフトプログラム、任意のプログラムソフトなどの配信システムとして使用してよい。

【0082】

【発明の効果】このように本発明によれば、受信機より後段の処理装置として標準的な装置を使用しながら、コンテンツオーナーが直接、所望のコピーコントロールを行なうことができるコンテンツ配信システムおよびコンテンツ配信方法を提供することができる。また、そのようなコンテンツ配信システムにおいて用いられ、配信されるコンテンツデータを受信し適切な権利処理を行なって利用可能に出力するデータ受信装置を提供することができる。また、コンテンツの権利者がその利用をコントロールできる状態で配信対象のコンテンツデータを提供するデータ提供装置およびデータ提供方法を提供することができる。さらに、そのように提供されたデータを送出するデータ送出装置を提供することができる。

【図面の簡単な説明】

【図 1】図 1 は、本発明の一実施の形態のコンテンツ配信システムの全体概略構成を示す図である。

【図 2】図 2 は、図 1 に示したコンテンツ配信システムの第 1 の具体例の主要部の構成を示す図である。

【図 3】図 3 は、図 1 に示したコンテンツ配信システムの第 2 の具体例の主要部の構成を示す図である。

【図 4】図 4 は、図 1 に示したコンテンツ配信システムの第 3 の具体例の主要部の構成を示す図である。

【図 5】図 5 は、図 4 に示したセットトップボックスの判定制御装置における判定処理を説明するためのフローチャートである。

【図 6】図 6 は、図 1 に示したコンテンツ配信システムの第 4 の具体例の主要部の構成を示す図である。

【図 7】図 7 は、図 6 に示したセットトップボックスの判定制御装置における判定処理を説明するためのフローチャートである。

【図 8】図 8 は、図 1 に示したコンテンツ配信システムの第 5 の具体例の主要部の構成を示す図である。

【図 9】図 9 は、図 1 に示したコンテンツ配信システムの第 6 の具体例の主要部の構成を示す図である。

【図 10】図 10 は、従来のコンテンツ配信システムの全体概略構成を示す図である。

【図 11】図 11 は、図 10 に示したコンテンツ配信システムの第 1 の具体例の主要部の構成を示す図である。

【図 12】図 12 は、図 11 に示した放送事業者で付加する制御記述子の具体例を示す図である。

【図 13】図 13 は、図 10 に示したコンテンツ配信システムの第 2 の具体例の主要部の構成を示す図である。

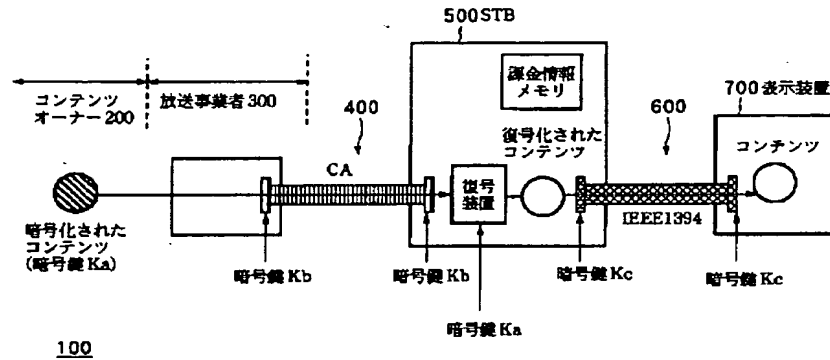
【符号の説明】

100…コンテンツ配信システム、200…コンテンツオーナー、208…電子透かし重畳部、210…暗号装置、212…制御記述子付加部、300…放送事業者、302…暗号装置、306…制御記述子付加部、400…放送網、500…セットトップボックス、502…復号装置、504…復号装置、506…電子透かし検出

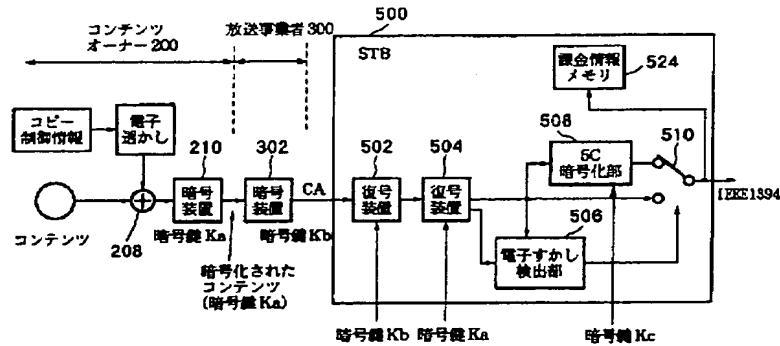
部、508…5C暗号化部、510…出力スイッチ、512…制御記述子検出部、514…判定制御装置、516…制御記述子1検出部、518…アナログ信号エンコーダ、520…暗号化部、522…アナログ出力スイッチ、524…課金情報メモリ、600…表示装置1/F、700…表示装置、911、912…コンテンツ配*

* 信システム、920…コンテンツオーナー、930…放送事業者、932…制御記述子付加部、934…暗号装置、940…放送網、950…セットトップボックス、952…復号装置、954…制御記述子検出部、956…5C暗号化部、958…出力スイッチ、970…表示装置

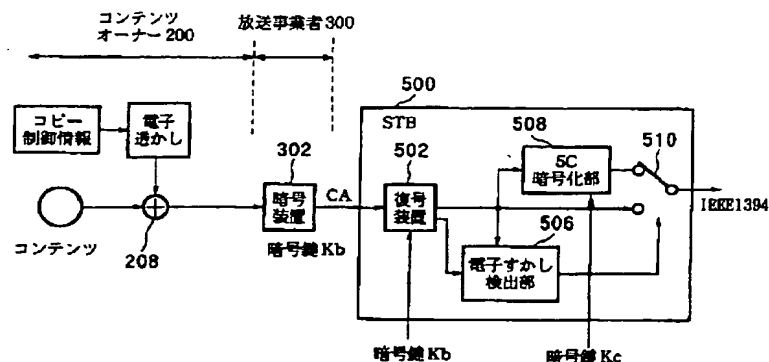
【図1】



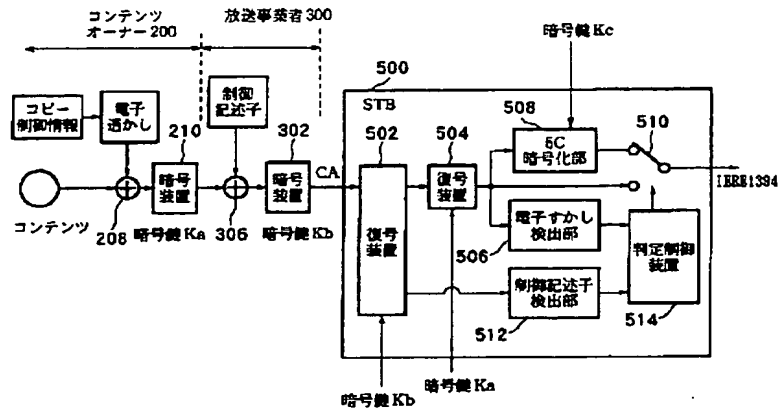
【図2】



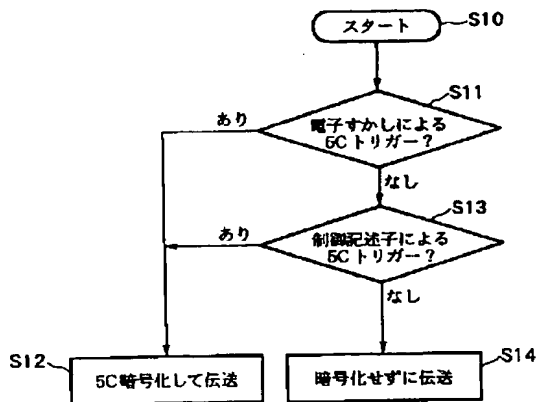
【図3】



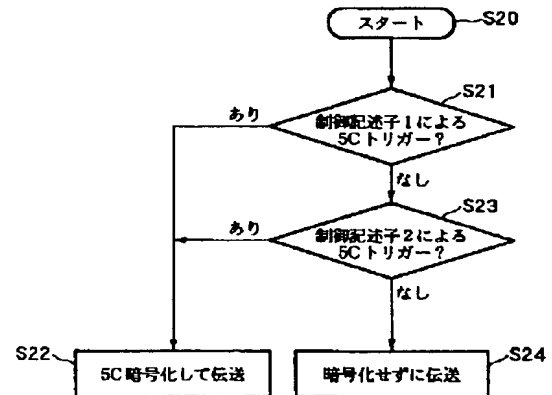
【図4】



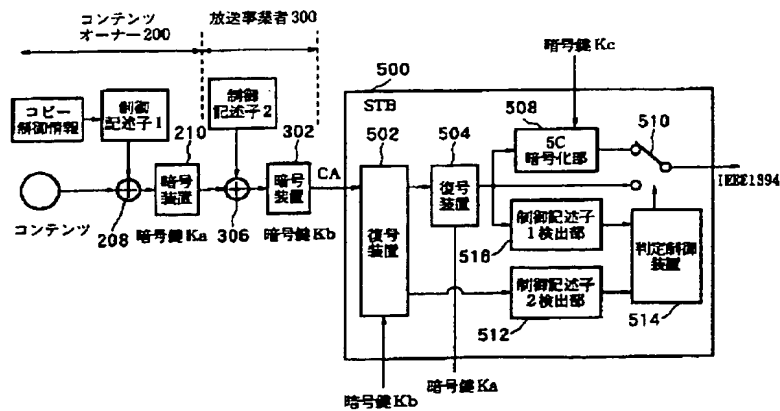
【図5】



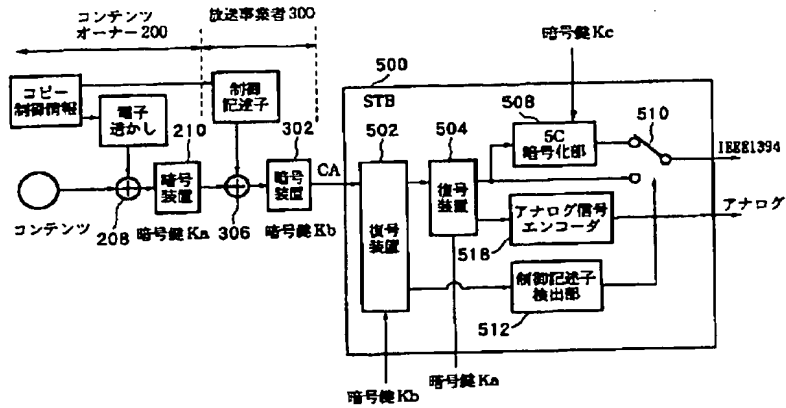
【図7】



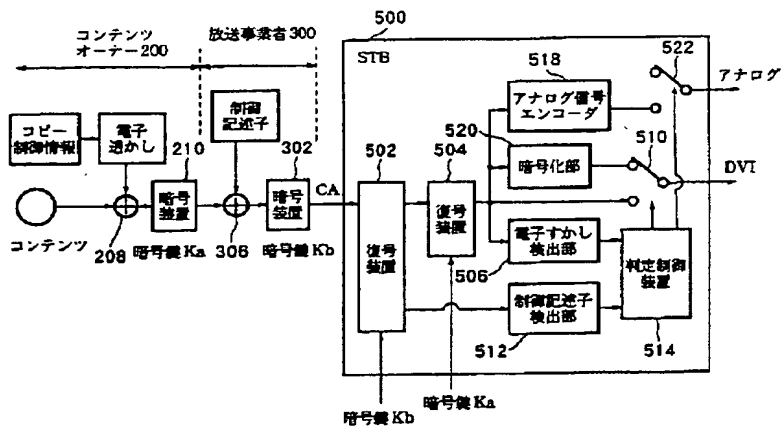
【図6】



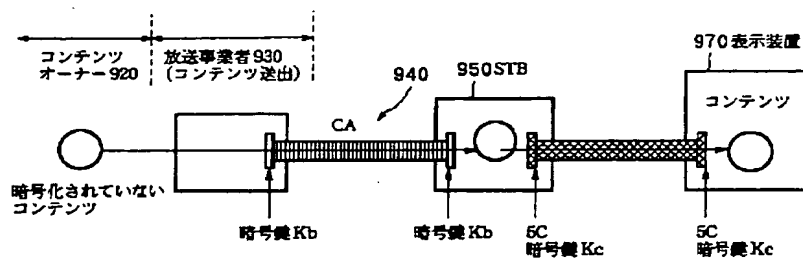
【図 8】



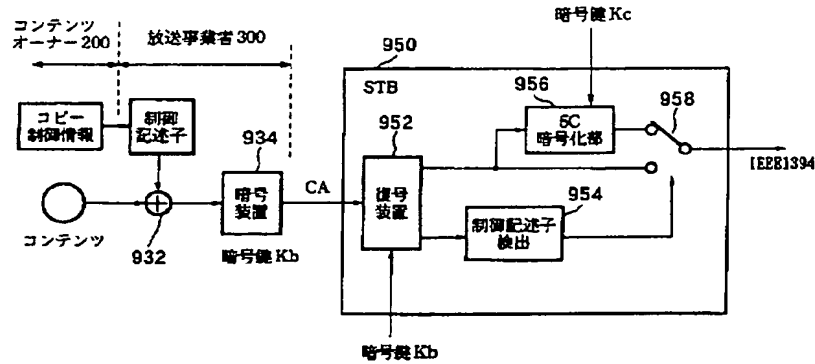
【図 9】



【図 10】



【図11】



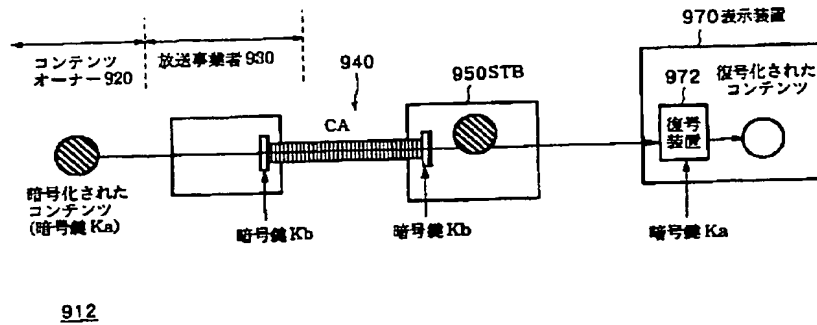
【図12】

```

digital_copy_control_descriptor 0 {
    descriptor_tag
    descriptor_length
    digital_recording_control_data
    maximum_bit_rate_flag
    component_control_flag
    copy_control_type
    if(copy_control_type == 01) { ← (1) 5Cを選択
        APS_control_data
    }
    else {
        reserved_future_use
    }
    if(maximum_bit_rate_flag == 1){
        maximum_bit_rate
    }
    if(component_control_flag == 1){
        component_control_length
        for(j=0;j<N;j++) {
            component_tag
            digital_recording_control_data ← (2) CGMSを伝送
            maximum_bitrate_flag
            reserved_future_use
            copy_control_type
            if(copy_control_type == 01){
                APS_control_data
            }
            else {
                reserved_future_use
            }
            if(maximum_bitrate_flag == 1){
                maximum_bitrate
            }
        }
    }
}

```

【図13】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)	
H O 4 N	5/44	H O 4 N	5/44	A
	7/08		7/08	Z
	7/081		7/167	Z
	7/167			

F ターム (参考) 5C025 BA25 DA01 DA04 DA05
 5C063 AA01 AB03 AB05 AB09 AC01
 CA12 CA23 CA36 DA07 DA13
 5C064 CA14 CB01
 5D044 BC03 CC04 DE42 DE49 DE50
 GK17 HL08 HL11
 5J104 AA01 AA14 BA03 PA04 PA06